A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid

Hairong Qi, *Senior Member, IEEE*, Xiaorui Wang, *Member, IEEE*, Leon M. Tolbert, *Senior Member, IEEE*, Fangxing Li, *Senior Member, IEEE*, Fang Z. Peng, *Fellow, IEEE*, Peng Ning, *Member, IEEE*, and Massoud Amin, *Senior Member, IEEE*

***Abstract*—Energy infrastructure is a critical underpinning of modern society that any compromise or sabotage of its secure and reliable operation has an enormous impact on people's daily lives and the national economy. The massive northeastern power blackout of August 2003 and the most recent Florida blackout have both revealed serious defects in both system-level management and device-level designs of the power grid in handling attacks. At the system level, the control area operators lack the capability to 1) obtain *real-time status information* of the vastly distributed equipment; 2) respond *rapidly enough* once events start to unravel; and 3) perform *coordinated actions autonomously* across the region. At the device level, the traditional hardware lacks the capability to 1) provide reliable frequency and voltage control according to system demands and 2) rapidly *reconfigure* the system to a secure state through switches and power-electronics based devices. These blackouts were a wake-up call for both the industry and academia to consider new techniques and system architecture design that can help assure the security and reliability of the power grid. In this paper, we present a hardware-in-the-loop reconfigurable system design with embedded intelligence and resilient coordination schemes at both local and system levels that would tackle the vulnerabilities of the grid. The new system design consists of five key components: 1) a location-centric hybrid system architecture that facilitates not only distributed processing but also coordination among geographically close devices; 2) the insertion of *intelligence* into power electronic devices at the lower level of the power grid to enable a more direct reconfiguration of the *physical* makeup of the grid; 3) the development of a robust collaboration algorithm among neighboring devices to handle possible faulty, missing, or incomplete information; 4) the design of distributed algorithms to better understand the local state of the power grid; and 5) the adoption of a control-theoretic real-time adaptation strategy to guarantee the availability of large distributed systems. Preliminary evaluation results showing the advantages of each component are provided. A phased implementation plan is also suggested at the end of the discussion.**

***Index Terms*—Adaptive algorithm, fault tolerance, hybrid systems, information security, power system security, reconfigurable architectures, robustness.**

Manuscript received October 21, 2010; revised April 21, 2011; accepted June 05, 2011. Date of publication August 30, 2011; date of current version November 23, 2011. This work was supported in part by National Science Foundation under Grant CNS-0716492 and CNS-0831466. Paper no. TSG-00196-2010.

H. Qi, X. Wang, F. Li, and L. Tolbert are with the Electrical Engineering and Computer Science Department, University of Tennessee, Knoxville, TN 37996 USA (e-mail: hairong.qi@gmail.com).

F. Z. Peng is with the Electrical and Computer Engineering Department, Michigan State University, East Lansing, MI 48824 USA.

P. Ning is with the Computer Science Department, North Carolina State University, Raleigh, NC 27695 USA.

M. Amin is with the Electrical and Computer Engineering Department, University of Minnesota, Minneapolis, MN 55455 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2011.2159819

I. Introduction

POWER SYSTEMS have widely dispersed assets that cannot be absolutely defended against a determined, coordinated attack [1]. There have been heightened concerns over the security of America's power grid. As early as 1997, basic security flaws had already been found in the computerized systems that control generators, switching stations and electrical substations [2], reported through a six-month vulnerability assessment conducted by the White House's National Security Telecommunications Advisory Committee. In 2007, an experimental cyberattack [3] run by the Department of Energy was mounted against a power generator, causing it to self-destruct. The most recent news report [4] is about detected signs (software signatures) made by hackers who had penetrated the computer systems that control the power grid. The terrorist attacks of 11 September 2001 have exposed critical vulnerabilities in America's essential infrastructures: Never again can the security of these fundamental systems be taken for granted.

In the 1999 report issued by the Electric Power Research Institute (EPRI), it is stated that the reliability of America's power grid is increasingly threatened while the technologies needed to counter the threat are delayed [5]. In 2005, NSF funded the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) Cyber Trust Center [6], conducting research to significantly improve the way the power grid is built, making it more secure, reliable, and safe. The TCIP project addresses the critical issues on protecting the information flow within the power grid. However, how to ensure the availability of the power grid in the presence of attacks is not fully examined. For example, if some critical devices are physically destroyed or completely controlled by inside attackers, the power grid will not function correctly. As another example, the trustworthy data communications and control components in TCIP rely on trustworthy data aggregation to make correct decisions. Detection of attacks or failures will have to be delayed until a relatively high level in the system, resulting in unnecessary delays.

In January 2010, the same team was awarded the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center [6] by the Department of Energy (DOE) with contributions from the Department of Homeland Security (DHS). In this new phase of development, the practice of cybersecurity has been expanded beyond just communication security and include, for example, data management security and device security. In addition to the TCIPG Center, North Carolina State University's Future Renewable Electric Energy Delivery and Management Systems (FREEDM) Center [7] also has a strong thrust in communication security.

Realizing the importance and challenges of cybersecurity in the power grid, especially with the dramatically escalated interests in smart grid development, DOE has recently announced the investment of more than $30 million for ten projects to address cybersecurity issues facing the nation's electric grid [8].

With the recent surge in smart grid study to improve the efficiency and availability of power, security has become one of the key issues brought to the front of the power grid innovation, as the addition of more monitoring and control capabilities has made the grid more prone to cyberattacks [9]–[15]. The unique features of the smart grid communication and control system call for a redesign of traditional network security approaches [16]–[23] as well as tailored security management and authentication approaches [24]–[29]. In addition, the deployment of advanced technologies like advanced metering infrastructures (AMIs) [30]–[34], wireless sensor networks [35] for better monitoring capability, and cloud computing [36] will introduce additional vulnerabilities to the grid and needs innovative and reliable solutions.

In this paper, we present a hardware-in-the-loop reconfigurable system with embedded intelligence and resilient coordination schemes at both local and system levels that would tackle the vulnerabilities of the grid. The system differentiates itself from previous and existing research efforts in the following key aspects. First, it features a location-centric hybrid system architecture which facilitates not only distributed processing but also coordination among geographically close (local) devices. The hybrid configuration would best prevent, detect, and mitigate faults, providing resilient reconfiguration capability through coordinated local actions. Second, the system pushes the intelligence toward the *lower level* of the power grid, allowing local devices to have the capability to make decisions and to react more quickly to contingencies, enabling a more direct reconfiguration of the *physical* makeup of the grid, as compared to current (e.g., software-only) approaches. Third, in order to improve the accountability of local decisions, a robust collaboration algorithm among neighboring devices is developed to handle possible faulty, missing, or incomplete information. Fourth, to better understand the local state of the power grid, a distributed algorithm is developed that identifies malicious inputs and prevents the attack from propagating to the system level. Fifth, the system adopts control-theoretic real-time adaptation strategies for analytic assurance in providing desired dynamic responses to unpredictable system changes, for efficiently maintaining the availability of large distributed systems.

The outline of the paper is as follows. Section II discusses requirements or performance metrics for a secure power grid. Section III describes the threat model. Section IV presents technical approaches that enables a resilient and reconfigurable power grid. Finally, Section V discusses future work.

II. Requirements for a Secure Power Grid

The vulnerability of the power grid to potential attacks calls for a redesign of the grid security analysis at both the system level as well as the device level. Specifically, a secure power grid should satisfy the following:

Real time requirement. Many contingency events in the power grid have time scales of 0.1–10 s. Present power system control devices are difficult, insufficient, and inflexible for real-time control and reconfiguration. The current operating standard, in which data are collected every few seconds, the state estimator runs every five minutes, and the contingency analysis runs even less frequently, certainly cannot satisfy the "real time requirement." Some major factors that affect the implementation of real-time management include the large amount of raw data, the communication delay, as well as the time-consuming security analysis algorithms. In order to achieve real-time operations, real-time scheduling and routing algorithms need to be designed to guarantee end-to-end real-time response even when the system is under various resource disturbance conditions. In addition, distributed processing of security analysis algorithms needs to be carried out to contain raw data communications within local areas and more quickly generate system state information to help detect and mitigate faults before they propagate.

Grid responsiveness requirement. Responsiveness can be implemented at two levels, the system level and the device level. The device-level response occurs more quickly to emergencies and helps automatically maintain the equilibrium of power flow at the local level. On the other hand, the system-level response, although occurring at a slower pace, would help correct the inappropriate responses made at the local level and thus maintain the stability of the grid at a higher level.

One technology that can help to alleviate some of the difficulties in the present electric system and increase the responsiveness of the power grid is to embed intelligent controllers in power electronic devices such as flexible ac transmission systems (FACTS). The incorporation of FACTS devices with appropriate sensing and control functions can transform the electric grid into a reconfigurable power system where actions can be taken in *milliseconds* to control the flow of power and ensure high levels of reliability and quality in the power system. This reconfigurable power system would act like a network of high-speed valves that can instantaneously control the flow of current through the entire grid and limit fault current and prevent cascading failures. The power electronics-based power system control devices with embedded intelligence will not only modernize today's grid infrastructure but also serve as the first line of defense. In addition, control-theoretic adaptation strategies can be developed to provide dynamic responses to unpredictable changes at the system level as another line of defense.

Collaborative processing requirement. The power grid is a vast interconnected network, where coordination across the network, if any, happens on a slow time-scale. Distributed energy resources make it nearly impossible for any precise central control of large numbers of small generators. Information exchange among hundreds or even thousands of distributed generation centers instead of just among a handful of large utilities is a new challenge brought by deregulation. Moreover, if terrorists can exploit the weaknesses of centralized control, security would seem to demand that smaller and locally collaborative systems would become the system configuration of choice.

Fault resiliency requirement. "Fault" is two-fold: hardware faults and data faults (note that in this paper, we do not consider software faults). Under the situation of hardware faults due to, for example, system attacks and contingency, a portion of the power grid needs to be able to isolate itself from the remainder of the utility system and continue to function. Data faults could include missing data, incomplete data, and incorrect data inputs

caused by either hardware faults and hardware inefficiency or deliberate attacks to the communication link. Under these situations, the analysis algorithms need to be able to tolerate the imperfect data inputs and still generate a correct response. We refer to this property as *resiliency*.

III. Threat Model

In a large interconnected power system, security is primarily focused on transient and dynamic stability considerations and intentional attacks are going to fall within only a few domains of influence upon the grid. Many of the scenarios manifest as equipment failures caused by physical equipment damage/failures, interruption of communication network, and/or misfeeding of information.

On one hand, the physical interconnection can provide a check on the information system should communications be compromised. If system response based on received data is counter to expectations, a device may be able to conclude a security breach. Physical laws govern the power flow in the grid, and these cannot be compromised. For example, if control actions such as increasing reactive power output are observed to decrease voltage, then the observation is either erroneous or the system has reached such an extreme and unusual state that all normal control laws are no longer effective. In this way, control provides feedback for detecting and isolating an attack to the information flow.

On the other hand, power systems can also fail through the physical interconnection even if the communication system is secure. For example, a generator, or group of generators, whose controller has been compromised can act in a way to destabilize other units, say by excessive response to minor load fluctuations. Information feedback and collaboration with properly functioning generator units may allow the system to isolate the offending unit and the system to continue to operate. In this way, *both the physical system and the information system can act together to help assure system security*.

A. The Threat Model

For convenience, we refer to the entities in a power grid as *system components*. The adversary may certainly launch *external attacks* against the system. Specifically, the adversary may passively intercept the messages exchanged between the system components, actively inject forged messages, or modify messages being transmitted. However, we assume there are communication security mechanisms (e.g., message encryption and authentication) that can handle such threats to a certain extent. Moreover, the adversary may launch denial of service (DoS) attacks to disable some system components (e.g., physically destroy a power generator) or the communication between them (e.g., cut the transmission line, flood the system with a large number of messages).

The adversary may also attempt to delay the communication between system components, aiming at preventing them from meeting certain real-time requirements. However, we assume the adversary cannot disable/delay *all* the system components and communication channels. The adversary may also launch *insider attacks*. Specifically, the adversary may compromise and completely control some system components, and use them to attack the rest of the system. However, we assume the adversary cannot control *all* the system components. The adversary may partially compromise the communication security. For example, the adversary may learn the cryptographic keys shared between some devices and thus can forge malicious messages. However, we assume the adversary can compromise only a portion of the secure communication links. Table I lists some example attacks under our threat model.

TABLE I
Example Attacks

External attack	Communication attack	Intercept messages; launch DoS attacks to disable communication between system components.
	Component attack	Physical power equipment (generator or power lines) failure or damage.
Insider attack	Communication attack	Modify or drop transmitted messages; inject false messages; delay message transmission.
	Component attack	Generate false events; control compromised system components to perform arbitrary tasks, such as coordinated attacks from multiple substations.

It should be noted that conventional U.S. power system planning is typically performed with the consideration of possible $\mathrm{N}-1$ contingency events of intrinsic equipment failure, where $\mathrm{N}-1$ contingency means one component (or one set of closely related components) fails. Occasionally, some regions of the U.S. power system are designed to handle a few critical $\mathrm{N}-2$ or even $\mathrm{N}-3$ contingencies (i.e., simultaneous failures of 2 or 3 components) with the assistance of postcontingency remedial actions. Nevertheless, under the post-9/11 environment, simultaneous coordinated strikes become a realistic threat, which will lead to $\mathrm{N}-\mathrm{X}$ operations under emergency. This will put the interconnected power network in a greater danger that the original power system planner had never envisioned.

B. Multiple Lines of Defense

This paper studies a systematic solution to fault prevention, detection, and mitigation, providing multiple lines of defense that are specifically tailored for the power grid, with potential generalization to other complex systems.

First, although there might be different ways to attack the system, the net result is always reflected as voltage, current, and/or frequency changes. Accurately detecting this change (or potential fault) and making quick adjustments at each device level, before it unravels, provide the *first line of defense*. The incorporation of some advanced power electronic devices with appropriate sensing and control functions can transform the electric grid into a reconfigurable power system where actions can be taken in *microseconds*. *Second*, the practice of robust collaboration among neighboring devices and distributed processing schemes at the local level provide the *second line of defense* in its ability to prevent isolated attacks from propagation and detect and mitigate coordinated attacks. *Third*, a control-theoretic adaptation framework at the system level provides the *last line of defense*, protecting the system from collapse by desired dynamic responses with analytical assurance.

A location-centric hybrid system architecture is designed to facilitate the realization of fault prevention, detection, and mitigation at various levels with various degrees of collaboration.

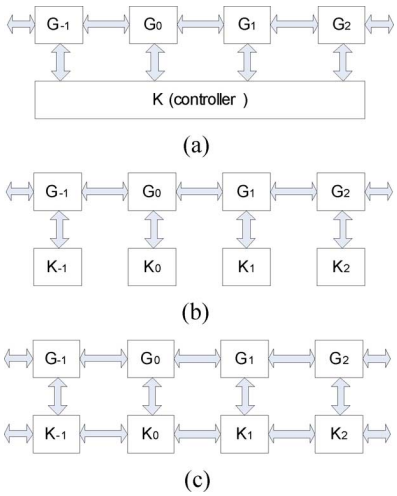

Fig. 1. A schematic illustration of different control strategies for a power grid defense system. K indicates centralized or local controller and G indicates the subsystem being sensed and actuated. (a) Centralized control. (b) Perfectly decentralized control. (c) Distributed control.

IV. Technical Approach

We present the design and development of a secure reconfigurable system supported by fault-resilient real-time controls to quickly respond to both natural and intentional attacks to the power grid. We expect a resilient reconfigurable power grid to incorporate both *local actuation, supported by devices with embedded intelligence*, and *central system-level adaptation, supported by control-theoretic security solutions*.

A. Location-Centric Hybrid System Architecture

Much of the vulnerability of the existing power grid can be traced to operating near the maximum voltage stability limits which does not allow the grid to respond quickly to adverse events at *centralized control* points [Fig. 1(a)] due to constraints on available information, communication bandwidth, and delay.

The alternative is a *perfectly decentralized control* strategy [Fig. 1(b)], in which local closed-loop command and control functions are implemented within each facility. Although data can be obtained in real time and actions can be enforced upon the local subsystem, the lack of information exchange between local controllers affects their capability to fully predict the effects of control actions, resulting in unreliable or biased decision making, affecting the stability of the power grid.

Yet another alternative is to allow coordination among geographically close (local) controllers, referred to as a *distributed control* scheme [Fig. 1(c)]. In this scheme, distributed controllers exchange information with key peers to ensure the reliability and safety of local operations, while coordinating strategies with more centralized command and control at a higher level in a hierarchical structure. The growth in dispersed power generation, transmission, and distribution equipment owned by multiple independent entities makes this distributed command and control structure essential. The threat of coordinated terrorist acts against the power grid leaves a coordinated distributed command and control solution as the only viable option.

In the following, we first examine the existing power grid infrastructure which basically adopts a centralized control scheme. As shown in Fig. 2(a), from top to bottom, the control

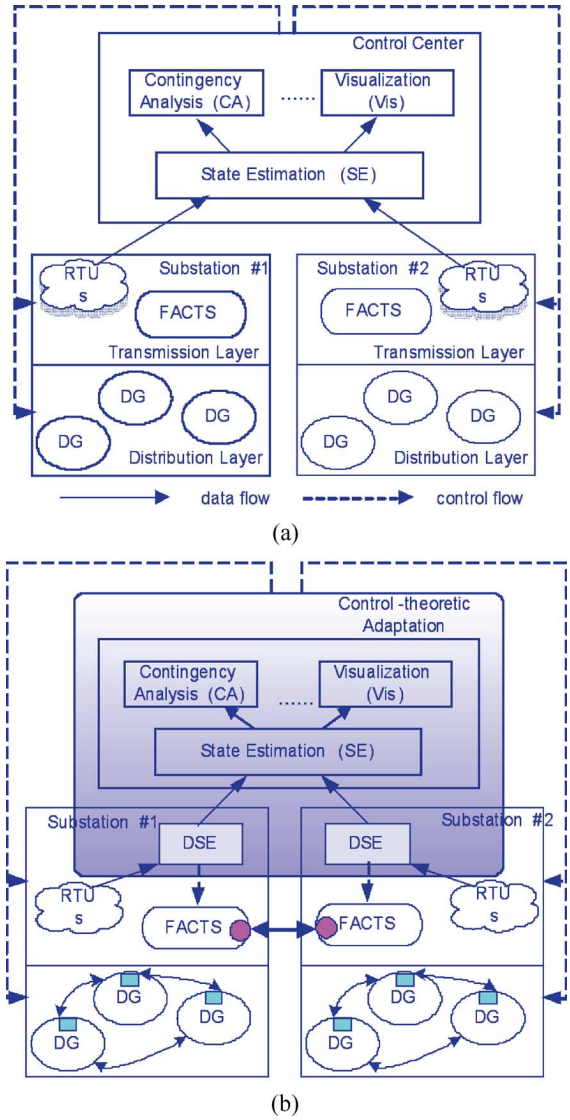

Fig. 2. System architecture of the power grid information management—a comparison. (a) Centralized architecture. (b) Location-centric hybrid architecture where filled circles and squares indicate embedded controllers.

center hosts critical power security analysis modules, such as contingency analysis (CA), visualization, etc., based on the input from the state estimation (SE) module, which, in turn, processes raw data sent from remote terminal units (RTUs) located at various substations. The control center also issues commands to adjust behaviors of local power electronic devices, including FACTS and distributed generators (DGs). Since there is *no* direct communication between substations, a FACTS device can only make isolated decisions even though it is equipped with the communication capability to respond to the control center. Similarly, at the distribution layer, where multiple DGs usually reside and are equipped to respond to the microgrid energy manager, there is no communication among DGs, let alone DGs across different substations.

Fig. 2(b) illustrates the proposed *location-centric hybrid* architecture, for a reformed power grid, which supports the distributed control scheme in Fig. 1(c). It differs from the existing power grid in four aspects. *First*, both FACTS and DG are embedded with an intelligent controller that makes decisions based on collaborative information from critical peers. *Second*, two

levels of collaborations are enabled, one is among DGs within the same area, the other is among FACTS devices across geographically adjacent substations. The location-centric collaboration provides effective mechanisms for preventing isolated attacks and detecting and mitigating coordinated attacks. *Third*, the SE module is not run at the control center. Instead, a distributed execution of SE (DSE) is performed at each substation, only the results from which are integrated at the control center. This way, the time- and resource-consuming SE execution can be distributed to multiple substations and the DSE module could provide feedback to local devices to contain faults locally before the system unravels. *Finally*, a control-theoretic adaptation scheme is adopted to help maintain grid stability under attacks, providing another level of protection of the grid.

In the following, we detail the enabling techniques that include embedded intelligence in hardware, robust local collaboration algorithm, distributed state estimation, and control-theoretic adaptation for system changes.

B. Reconfiguration Through Hardware Reactivity with Embedded Intelligence

As stated in Sections II and III, the incorporation of some advanced power electronic devices with appropriate sensing and control functions can transform the electric grid into a reconfigurable power system where actions can be taken in *microseconds*. In this section, we describe the functionality of two such devices, FACTS and DG, and how to design a local controller to be embedded in these devices in the context of a specific application.

One important concept to clarify first is the capability and necessity of these devices in supplying *reactive* power. Reactive power control and management is extremely important to voltage stability/control and high efficiency [37]. Large reactive power flows were a contributing cause to the line overloads that initiated the cascading blackout in August 2003 [38]. Although it does not perform real work or help transfer power, reactive power is needed to help regulate the voltage throughout the electric grid. Reactive power is much more valuable if it is supplied *locally* where it is needed, otherwise, the current associated with it would cause additional system losses and reduce the efficiency and real power capacity of the system. In other words, the ultimate goal of the intelligent controllers is to decide how much reactive and real power to be injected to the grid under certain change detection (in voltage, current, or frequency) made at the devices. In the following, we discuss the design of such a controller under the context of *intentional islanding*.

Intentional islanding is a condition in which a microgrid or a portion of the power grid, which contains both load and distributed generation (DG), is isolated from the remainder of the utility system (or main grid) and continues to operate. Intentional islanding is important for microgrids to continue to provide power to sensitive loads under system attacks and contingency. During the normal grid connected operation, each DG in a microgrid usually operates in the *current (or power) control mode* in stiff synchronization with the main grid. When the microgrid is cut off from the main grid or when main power outage occurs because of system component attacks, each DG has to detect this islanding situation and has to be *switched to a voltage control mode* to provide constant voltage to local

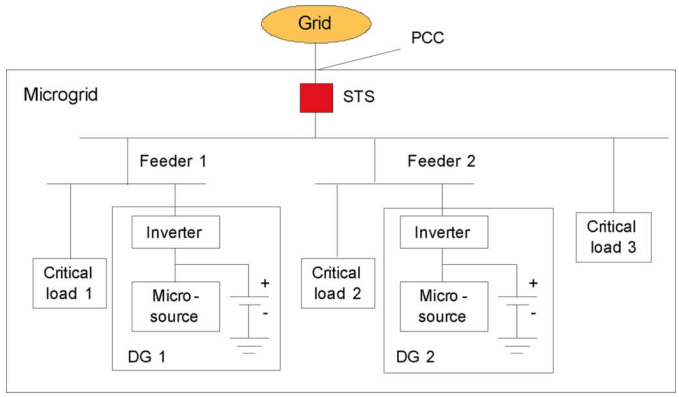

Fig. 3. A microgrid with 2 DGs.

sensitive loads. Since the local DG is either less or greater than local load demand, *intelligent* load shedding is needed for intentional islanding operation, which makes it essential to search for an analytical solution of the voltage and frequency transients locally for each DG to have information and make decisions to secure energy delivery to sensitive loads. This is the principle in designing the intelligent controller embedded at DG [39].

Fig. 3 illustrates a microgrid with 2 DGs and 3 critical loads. In order to maintain the microgrid's operation after main power outage, the total amount of active and reactive power needed by the load, $\Sigma P_L = P_{L1} + P_{L2} + P_{L3}$ and $\Sigma Q_L = Q_{L1} + Q_{L2} + Q_{L3}$, and the total amount of active and reactive power generated by the DGs, $\Sigma P_G = P_{G1} + P_{G2}$ and $\Sigma Q_G = Q_{G1} + Q_{G2}$ need to be balanced and satisfy $\Sigma P_L = \Sigma P_G$ and $\Sigma Q_L = \Sigma Q_G$.

When the voltage at the point of common coupling has dropped to less than 0.88 pu or increased to greater than 1.1 pu, the main power grid is deemed as outage of service according to the IEEE Std. 1547. The challenge is how to switch the DG inverter system to voltage control mode and bring the voltage back to within the normal range (0.88–1.1 pu) for intentional islanding operation.

Fig. 4 shows the theoretical voltage transients for a constant impedance load under various power differences (from -50% to $+50\%$) after main power outage. We observe that the voltage change rate is closely related to power differences between the DG and load demand. This has presented a potential solution that if we can detect the voltage change rate and profile after the power outage, we can then determine how much load shedding or how much generation reduction is needed before going to the intentional islanding operation and switching to the voltage control mode. This operation can be conducted at the *local* DG level based on *local* voltage and frequency monitoring and state estimation for faster responsiveness to system state changes.

We have successfully field-tested this on a simple microgrid system with one DG and local loads, connecting to the main power grid which is under attack [40]. However, when there is more than one DG in the microgrid which is normally the case, the DG controller would fail because of the lack of information exchange among the DGs, causing an inaccurate estimate of the state of the microgrid. The robust local collaboration algorithm and distributed state estimation to be discussed in the next two sections provide effective solutions to this problem.

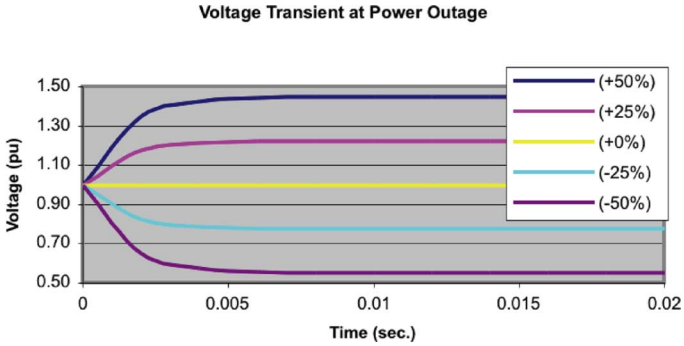

Fig. 4. Voltage transients of constant impedance load during main power outage.

C. Interval-Based Robust Local Collaboration

When a controller embedded in a power electronic device detects a change in the power grid or receives an update message from the low-level controllers, a reactive action will take place. Very often, the controller's own knowledge is not enough to make a valid decision which is when the location-centric peer-to-peer coordination is initiated, as structured in Section IV-A. In other cases, the communication links to one or several controllers from the field RTUs can be jammed or damaged, or the RTUs themselves are compromised, resulting in missing data, incomplete data entries, or even worse, incorrect data. Under these circumstances, the local controllers need to be able to make correct decisions that do not jeopardize grid stability or reliability. We develop a generic algorithm to achieve fault resiliency (or fault prevention, detection, and mitigation) based on multiple controller coordination even with potentially faulty, incomplete, and missing information. This will be realized by the development of an *interval-based* sensor data integration algorithm.

Different from the *value-based* integration based on inputs from devices which, without loss of generality, assumed to be concrete numbers, the interval-based integration takes in an input and creates an interval clustered around the physical readout. The *interval estimate* can be modeled by different stochastic distributions, the simplest of which would be a uniform distribution. Based on this definition, a *correct device* is one whose interval estimate contains the actual value of the parameter being measured. Otherwise, it is a faulty device. For example, in the case of collaborative intentional islanding, a DG might receive a reading from a power line that indicates its overloading condition, e.g., 25% overloaded, yielding an interval of [20%, 30%] modeled by a Gaussian, in which we interpret the interval as "The power line is 20% to 30% overloaded."

In order to integrate the interval measurements from different controllers, we develop a *distributed interval integration algorithm* [41], [42], derived from its original centralized version [43], in which a local device, like DG, is elected to collect the outputs of the devices and construct an *overlap* function. Fig. 5 illustrates the construction of an overlap function for a set of 6 devices. We observe that the actual value of the derived information lies within regions, referred to as the "crest" over which the maximal peaks of the overlap function occur with the largest spread. In Fig. 5, the crest picked would be $[A, B]$. In [43], the

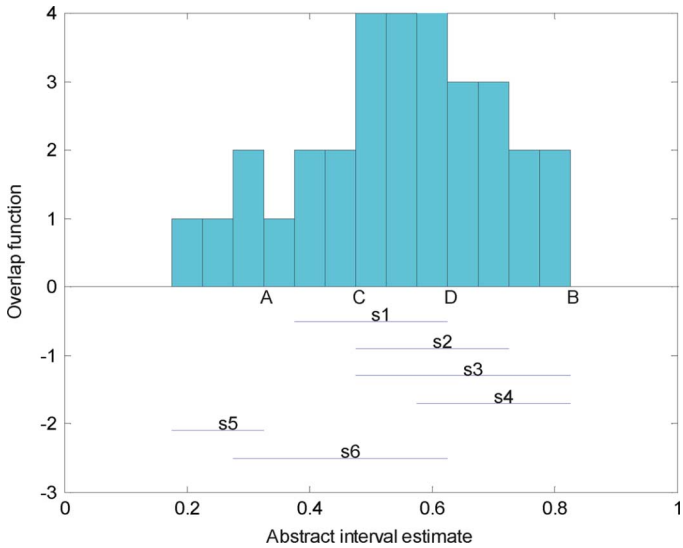

Fig. 5. The overlap function constructed from six devices.

authors show that the algorithm is robust and satisfies a Lipschitz condition [44], which ensures that minor changes in the input intervals cause only minor changes in the integrated result. We have improved the integration algorithm to only return the interval ranges $[n–f, n]$ where f is the number of faulty device inputs and n is the total number of sensors. In Fig. 5, among the $n = 6$ devices, there are $f = 2$ faulty devices. Thus the final integration result will be $[C, D]$ where the overlap function has the range [4, 6]. This algorithm also satisfies Lipschitz condition and its main advantage is that it is able to reduce the width of the output interval in most cases and produce a narrower output interval when the number of devices involved is large. According to the Byzantine generals problem, the maximum number of faults (f) that a certain amount of devices (n) can tolerate is the largest integer that is smaller than $(n-1)/3$. We have developed a set of criteria for local controllers to jointly reach a consensus decision [41], [45].

In order for the controller to automatically determine when it can stop the integration process, we use $c = h \times w \times acc$ to pick the "*crest*" where h is the height of the highest peak in the overlap function, w is the width of the peak, and acc is the estimate at the center of the peak. The peak with the largest c is selected as the crest. This "*intermediate accuracy*" c can then be used to determine if the controller has achieved the required accuracy (or the decision is valid) or not. We design a *protocol* for assisting the decision making process. If and only if the following three criteria are satisfied, the local controller has to continue collaboration with its neighbors to obtain more information, that is, the controller's decision is not reliable enough to be trusted.

1) The overlap function has its highest peaks ranging from $[n–f, n]$.
2) The center of the integration result has to be equal to or larger than the median of the estimated interval. For example, if the estimated interval is [0, 1], then the integrated accuracy cannot be less than 0.5.
3) Both 1 and 2 have to be satisfied in two adjacent integrations excluding the first trial in order to add stability to the decision.

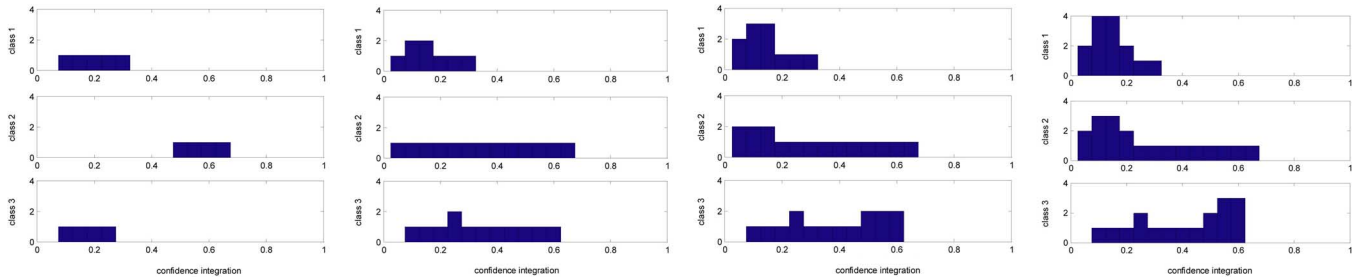

Fig. 6. Multiple controller interval integration results with a progressively improving reliability (From left to right: DG1, DG1+2, DG1+2+3, DG1+2+3+4).

DGs	Line #1	Line #2	Line #3
1	[0.10, 0.29]	[0.46, 0.65]	[0.10, 0.21]
2	[0.05, 0.14]	[0.05, 0.41]	[0.22, 0.58]
3	[0.05, 0.15]	[0.05, 0.15]	[0.49, 0.59]
4	[0.08, 0.16]	[0.08, 0.16]	[0.51, 0.60]

(a)

	DG1		DG1+2		DG1+2+3		DG1+2+3+4	
	c	*acc*	*c*	*acc*	*c*	*acc*	*c*	*acc*
Line #1	1	0.2	0.5	0.125	0.75	0.125	1	0.125
Line #2	**2.3**	**0.575**	**4.55**	**0.35**	0.6	0.1	0.75	0.125
Line #3	0.7	0.5	0.5	0.25	**3.3**	**0.55**	**3.45**	**0.575**

(b)

Fig. 7. The progressive controller decision-making process. (a) Initial decision by four neighboring DGs. (b) Collaboration results from controllers.

We provide an application example to show how this protocol is applied. Assume a neighborhood of four DGs participate in a collaborative decision making process in order to determine which power line is most overloaded. For example, upon receiving readings from power line #1, DG1 remodels it to be 0.10 to 0.29 overloaded, as shown in Fig. 7(a). In this example, DG1 provides a tamely faulty result. Fig. 6 illustrates how collaboration among local controllers generates the partially integrated estimate range when the integration is progressively performed from DG1 to DG4. The four subfigures show the intermediate results while the controllers perform integration. Fig. 7(b) summarizes the controller's decision making procedure after integration with each of its four neighbors. We observe that the integration result at DG1 and DG1+2 shows that "line #2" is the most overloaded but changes to "line #3" when integrating with inputs from DG3 and DG4.

D. Improving Computational Efficiency for State Estimation

Besides robust local collaboration, the existing power grid also provides security analysis algorithms run at the control center to best determine the status of the power grid. State estimation (SE) is one of such algorithms which is essentially the process of estimating unknown state variables in a power grid based on the meter measurements. However, existing computation is too time consuming. A natural way to improve computational efficiency and avoid "large system problems" is to use parallelism with distributed processing. The geographical distribution of power system applications can benefit from the form of a decentralized information architecture, in which several remote processors perform the local state estimation with the result forwarded to a control center to refine calculations. The output of distributed SE can be used by local controllers to better understand the state of the power grid. It can also provide feedback information to assist in fault detection when the expected state is very different from the estimated state.

There exist a number of parallel and distributed state estimation algorithms [46], [47]. In most approaches, the problem is formulated as follows: the network is divided into several small areas, a local optimal estimation problem is formulated on each smaller area and constraints are put on the boundary buses to ensure the consistency of the bus states. This results in a class of *synchronous* methods, since each iteration of a local state estimation requires the iteration result of other areas.

We develop an *asynchronous* distributed algorithm whose objective is to combine the existing conventional state estimation and at the same time introduce distributed processing to take advantage of today's improved communication capacity and increase in sensors. In the new algorithm, the network is partitioned into a large number of overlapping areas. Each area has its own local processor which subscribes to the measurements published for its area and performs an approximate local state estimation. These areas will have significant **overlap** with each other, not just on the boundary buses as typical of most of the other distributed state estimation. The overlapping areas serve two purposes. One is that the results from two different local estimators on the overlapping area can be used in the final stage to reduce the discrepancy and consolidate results. The other is to avoid the difficulties in bad data detection and identification near/on the boundary buses as in traditional distributed state estimation. Each area performs its own state estimation individually with the iteration occurring both spatially and sequentially until the result converges into a desired tolerance. The result can be passed to a central processor or used locally for fast control actions.

We have performed a study to evaluate the distributed SE on the IEEE 30-bus system. A comparison of the results from the distributed state estimation and traditional whole network state estimation shows a slight increase in mean squared error (MSE) [48], [49]. This is to be expected as the local estimates are not a global optimization and do not have full network information. Moreover, it is completely scalable as system size increases and can easily incorporate more local measurements that are not included in this simple test.

E. Control-Theoretic Adaptation to System Changes for Real-Time Guarantee

A power grid system must be capable of adapting to unpredictable changes or security attacks (e.g., when the attacks have penetrated the first two lines of defense) while continuing to operate effectively. To provide analytic assurance on desired dynamic response to quality-of-service (QoS) attacks, we

can define a *control-theoretic* framework based on advanced control theory such as model predictive control (MPC). Using this framework, we will model the system as a dynamic system whose controlled variables (e.g., QoS attributes like real-time response time, throughput) must track their references (e.g., QoS specifications). The impacts of QoS attacks on the system can be modeled as disturbances and system variations. When the disturbances occur, the power grid may experience abnormal current, voltage, and/or frequency that further cause equipment damage and failures. A *key benefit* of control-theoretic framework lies in well-established design methodologies and its ability to provide analytical performance assurance (e.g., system stability, speed of recovery from attacks, and system QoS in steady states after recovery) when workload and resource availability fluctuate unpredictably (e.g., as in the case of distributed denial-of-service (DDoS) attacks).

We develop novel real-time algorithms based on control theory to schedule different tasks in the system. The goal is to guarantee the end-to-end real-time deadlines of high-priority tasks even when the system is suffering resource contention caused by QoS attacks. For example, when the system is under attack, the tasks of alarm propagation, contingency analysis, and state estimation should have high priorities, and thus their resource requirements (i.e., CPU time or network bandwidth) have to be satisfied. In contrast, the tasks of data collection and backup can be temporarily suspended or run in much lower task rates. As a result, the system is able to execute the most important tasks and continue to be operational and available, even under security attacks.

To fulfill our goal, decentralized real-time scheduling algorithms can be designed based on recent advances in feedback control theory to provide a highly scalable solution in large-scale systems. We first focus on an important real-time scheduling approach called *utilization control*. The (CPU) utilization of a processor is the percentage of time when its CPU performs useful computation. The goal of utilization control is to enforce desired utilizations on one or more processors despite significant uncertainties in system workload. Utilization control is crucial to real-time systems because all tasks on a processor are guaranteed to meet their real-time deadlines if the utilization of the processor is equal to or lower than an appropriate schedulable utilization bound [50], [51]. Utilization control provides us an effective way to guarantee all real-time deadlines without the need to know the accurate workload details. It can also enhance system survivability by providing overload protection against workload fluctuation [52].

Utilization control can be formulated as a dynamic constrained optimization problem. Given the utilization set point vector, $\boldsymbol{B} = [B_1 \dots B_n]^T$ where B_i denotes the desired utilization on processor P_i, and a rate constraint $[R_{\min,i}, R_{\max,i}]$ for each task T_i, the controller dynamically chooses the task invocation rate $r_i\ (k)$ for each task to minimize the difference between the set point B_i and the utilization $u_i\ (k)$ for each processor in the system, subject to the rate constraint:

$$\min_{\{r_j(k)|1\le j\le n\}} \sum_{i=1}^{n} (B_i - u_i(k))^2$$
$$\text{subject to } R_{\min,j} \le r_j(k) \le R_{\max,j} \quad (1 \le j \le m)$$

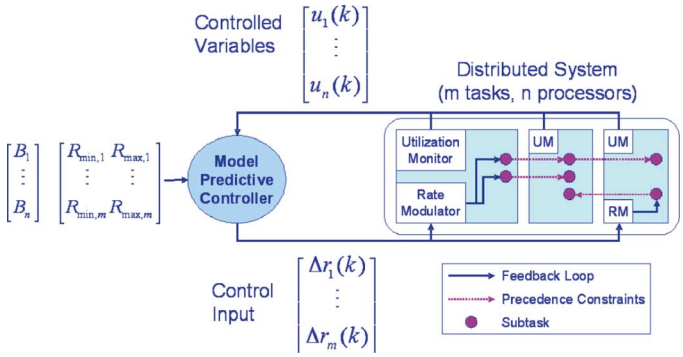

Fig. 8. The MIMO feedback control loop in EUCON.

The rate constraints ensure all tasks remain within their acceptable rate ranges. The optimization formulation maximizes task rates (and hence the system value, e.g., the frequency of state estimation) by making the utilization of each processor as close to its set point as allowed by the constraints. We have developed a centralized utilization control algorithm (EUCON—End-to-end Utilization CONtrol) for distributed real-time systems.

EUCON [53] is designed for end-to-end utilization control. It can maintain desired CPU utilizations on multiple processors despite uncertainties in task execution times and coupling among processors. It employs a centralized multi-input-multi-output (MIMO) controller based on model predictive control (MPC) theory to manage and coordinate the adaptation of multiple processors, subject to the constraints on task rates. As shown in Fig. 8, EUCON features a distributed feedback control loop composed of a central *controller*, and a *utilization monitor* and a *rate modulator* on each processor.

A decentralized end-to-end utilization control algorithm, DEUCON, has been developed. Compared to centralized control schemes, a fundamental advantage of DEUCON is that both the computation and communication overhead of a controller depend on the size of its neighborhood instead of the entire system. This feature allows DEUCON to scale effectively in large distributed real-time embedded systems such as the power grid. In addition, DEUCON can also tolerate considerable network delays, which makes it well suited to provide end-to-end real-time status dissemination in power grid systems. Based on EUCON and DEUCON, we plan to develop a feedback controlled middleware system running on QoS-critical security analysis modules. This middleware system can control desired QoS metrics such as end-to-end latency and resource utilization by adapting the task invocation rates and migrating tasks to different hosts in the system based on control-theoretic decisions.

We have also developed a resilient real-time middleware system called FC-ORB [52]. Empirical experiments show that FC-ORB can improve the fault-tolerance capabilities of QoS-critical systems by helping them survive malicious QoS attacks. Fig. 9(a) shows that the system successfully tolerates external resource contentions which occur on the four processors sequentially from processor 1 to processor 4 by maintaining the desired CPU utilizations. Such external disturbances may be caused by a variety of sources including i) processing of critical events that must be executed at the cost of other tasks; ii) varying workload from a different subsystem

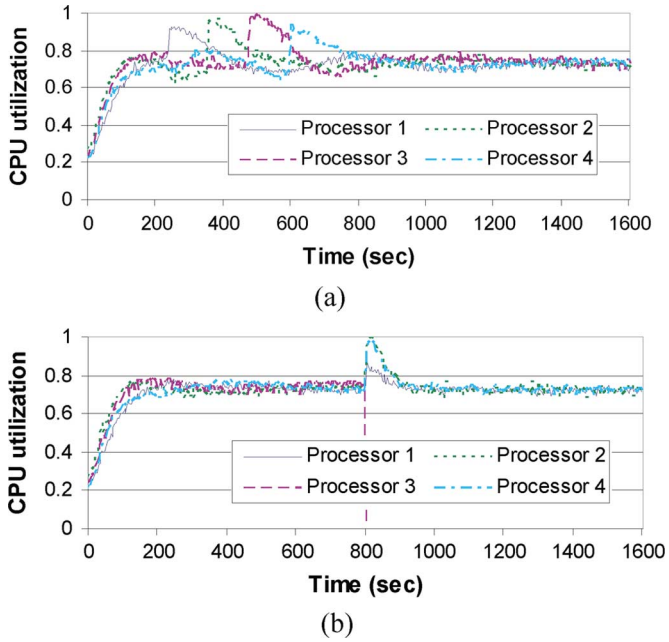

Fig. 9. CPU utilizations of all processors under (a) external disturbances and (b) processor failure.

(e.g., legacy software from a different vendor); and iii) software faults or adversarial denial of service (DoS) attacks. Fig. 9(b) shows that the failure of processor 3 at time 800 s triggers task migrations and then system overload. Due to the adoption of feedback control, possible cascaded processor failures are avoided by maintaining desired CPU utilizations. In both cases, as a result of utilization control, end-to-end real-time deadlines have been guaranteed [52].

V. Discussion

The power grid constitutes the fundamental infrastructure of modern society. A successful attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and the lives of every citizen. We have presented a location-centric hybrid system architecture as compared to the existing centralized architecture to facilitate the realization of fault prevention, detection, and mitigation at various levels with various degrees of collaboration, including local actuation, supported by devices with embedded intelligence, robust local collaboration, and distributed state estimation, as well as system-level adaptation, supported by control-theoretic security solutions. We presented enabling techniques at each level to demonstrate the effectiveness of the proposed architecture.

In the following, we discuss potential future works for these techniques as well as a phase implementation plan.

At the local actuation level, although we have discovered potential solutions to use DG to implement intentional islanding, it is only successful when there is just one DG in the microgrid. With multiple DGs as shown in Fig. 3, the potential solution would fail. The reason is that to maintain the functionality of the microgrid even after the main grid is under attack, not only the equilibrium between load generated and load consumed have to be satisfied in real time, the following two conditions have to be met: 1) the total apparent power demand has to be less than the current total DG apparent power capacity and 2) the powers drawn by the loads from each DG have to be limited within its capacity and available active power individually. The solution with one DG can only satisfy the first condition. In order to satisfy the second condition, coordination and exchange of information among the DGs in addition to power and frequency droop control are needed to obtain a comprehensive view of the system state.

However, the existing power grid does not provide communication capability among DGs, and if we open up the communication channel between DGs, it seems that we would also open up the system to intentional attacks, like injecting faulty data into the grid. To tackle these potential challenges, collaboration among geographical-close DGs is provided with robust integration algorithms in place to warrant its secure execution. Given that, more advanced controllers need to be designed to integrate distributed inputs and make a robust decision. On the other hand, with the flexibility of testing different functionalities of FACTS, the main challenge is to determine which function to switch to under what type of change conditions. This again needs coordination and information exchange and state estimation.

For robust local collaboration, the interval-based integration algorithm cannot be realized without a real-time communication protocol in place. The key issue in real-time communication is to meet the end-to-end deadlines of those contingency events and tasks. In real-time theory, an end-to-end real-time deadline can be divided into a set of local deadlines on each node that the events/tasks go through plus a set of network latencies between each two adjacent nodes. Therefore, the goal of meeting an end-to-end deadline is transformed to the problem of meeting each local deadline and guaranteeing the network latency of each link. We plan to monitor the latency between every two nodes in the system. When network latency is longer than the desired deadline (e.g., due to security attacks), three potential solutions have been discussed to achieve the desired latency for high-priority tasks. First, low priority traffic flows can be dropped or the quality of service (QoS) levels of low priority flows can be adapted to guarantee the latency of high priority packets. For example, image or video messages can be replaced with text messages. Second, novel QoS-aware routing algorithms can be developed so that packets with higher priorities can be processed in a timelier manner than those lower priority ones. Finally, malicious processes in the systems can be identified using advanced security approaches and then terminate those processes in the system.

Although we have provided preliminary evaluation results to each component except for the system architecture, a comprehensive evaluation of the new power grid architecture is essential. We are planning to use EPRI's dynamic security assessment (DSA) model to evaluate the system performance among three different control architectures, namely, centralized, perfectly decentralized, and distributed. Both top-down models and bottom-up models will be evaluated. Top-down models start from large-scale graphs and look at the interactions between components. Because there are so many components and potential interactions, deriving all-encompassing rules for complex infrastructures is impractical. Therefore, top-down models offer some insight but cannot adequately reflect real-world situations for complex infrastructures. We will develop a bottom-up model, specifically for the power industry which allows implementation for the individual parts of a system. By concentrating on smaller parts of the system, deriving rules becomes more

practical, where real-world complexity is modeled by letting the individual controller interact independently, as opposed to the centralized control inherent in top-down models.

In addition to software-based simulation, work is underway to emulate threat models and demonstrate the effectiveness of the system architecture using NextEnergy's microgrid developed in partnership with DTE Energy Technologies.

To implement the proposed architecture of a future resilient power grid, an incremental deployment is suggested since a total replacement can be hardly justified economically. The discussion below shows a sample implementation strategy using the bottom-up approach, although other variations may work as well.

First, the local intelligence among DGs and FACTS devices can be implemented as a response to observed local variables such as voltage, current, and power. Here, trending analysis using local variables can be an integrated part for making local decisions.

Then, communications and collaborative intelligence can be implemented among local devices such that decisions can be made based on nearby information. An example is distributed state estimation with input from nearby devices but not global information. Real-time guarantees can be a critical task to implement coordination among peers. The implementation in this stage broadens the scope of information utilization and reaches an improved decision as opposed to purely localized decision making.

Finally, the communication and coordination can be fully expanded to link the centralized control center and downstream devices. Therefore, global decisions can be made when there is enough time to reach such decision to optimize the daily operation. Meanwhile, emergency decisions can be quickly made using local information as well as nearby communication to avoid a global instability or collapse.

REFERENCES

[1] M. Amin, "Energy infrastructure defense system," *Proc. IEEE*, vol. 93, no. 5, pp. 861–875, May 2005, Special Issue on Energy Infrastructure Defense Systems.

[2] K. Poulsen, "Sparks over power grid cybersecurity," *SecurityFocus* Apr. 10, 2003 [Online]. Available: http://www.securityfocus.com/news/3871

[3] J. Meserve, "Staged cyber attack reveals vulnerability in power grid," CNN Rep., Sep. 26, 2007 [Online]. Available: http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US

[4] B. Ghosh, "How vulnerable is the power grid?," *Time* Apr. 15, 2009 [Online]. Available: http://www.time.com/time/nation/article/0,8599,1891562,00.html

[5] EC&M Staff, "How reliable is our electricity?," *Electr. Construction Maintenance* Dec. 1, 1999 [Online]. Available: http://ecmweb.com/mag/electric_reliable_electricity/

[6] "TCIP: Trustworthy cyber infrastructure for the power grid," [Online]. Available: http://tcipg.org

[7] FREEDM, "Future Renewable Electric Energy Delivery and Management Systems Center," North Carolina State Univ. Raleigh, NC [Online]. Available: http://www.freedm.ncsu.edu

[8] "Secretary Chu announces latest efforts to address cybersecurity," U.S. Dept. Energy, 2010 [Online]. Available: http://www.energy.gov/9539.htm

[9] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in *Proc. Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, 2008, pp. 1–5.

[10] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proc. Power Energy Soc. Gen. Meet.*, 2010, pp. 1–5.

[11] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. (ISGT)*, 2010, pp. 1–7.

[12] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[13] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[14] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[15] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "Trust infrastructures for future energy networks," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, 2010, pp. 1–7.

[16] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, 2010.

[17] R. Zhang, Z. Zhao, and X. Chen, "An overall reliability and security assessment architecture for electric power communication network in smart grid," in *Proc. Int. Conf. Power Syst. Technol. (POWERCON)*, 2010, pp. 1–6.

[18] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proc. Military Commun. Conf. (MILCOM)*, 2010, pp. 1830–1835.

[19] S. Hong and M. Lee, "Challenges and direction toward secure communication in the SCADA system," in *Proc. Annu. Commun. Netw. Serv. Res. Conf. (CNSR)*, 2010, pp. 381–386.

[20] J. Zhang and C. A. Gunter, "Application-aware secure multicast for power grid communications," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 339–344.

[21] T. M. Overman and R. W. Sackman, "High assurance smart grid: Smart grid control systems communications architecture," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 19–24.

[22] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. Innov. Smart Grid Technol. (ISGT)*, 2010, pp. 1–7.

[23] Y. Wang, I. R. Pordanjani, and W. Xu, "An event-driven demand response scheme for power system security enhancement," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 23–29, 2011.

[24] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Computer network security management and authentication of smart grids operations," in *Proc. Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, 2008, pp. 1–6.

[25] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Proc. Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, 2008, pp. 1–7.

[26] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore, and T. Andel, "Trust management and security in the future communication-based 'smart' electric power grid," in *Proc. 44th Hawaii Int. Conf. Syst. Sciences (HICSS)*, 2011, pp. 1–10.

[27] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber infrastructure authentication protocols," in *Proc. 43rd Hawaii Int. Conf. Syst. Sciences (HICSS)*, 2010, pp. 1–10.

[28] Z. Sun, H. Zhang, and J. Ma, "Key management for advanced power distribution system using EPON," in *Proc. Int. Conf. Crit. Infrastruct. (CRIS)*, 2010, pp. 1–5.

[29] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 327–332.

[30] D. P. Varodayan and G. X. Gao, "Redundant metering for integrity with information-theoretic confidentiality," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 345–349.

[31] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid M2M networks," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 333–338.

[32] C. Bennett and S. B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks," in *Proc. Innov. Smart Grid Technol. (ISGT)*, 2010, pp. 1–6.

[33] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 350–355.

[34] Y. J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 58–65, 2010.

[35] Y. Wang, W. Lin, and T. Zhang, "Study on security of wireless sensor networks in smart grid," in *Int. Conf. Power Syst. Technol. (POWERCON)*, 2010, pp. 1–7.
[36] Y. Wang, S. Deng, W. Lin, T. Zhang, and Y. Yu, "Research of electric power information security protection on cloud security," in *Int. Conf. Power Syst. Technol. (POWERCON)*, 2010, pp. 1–6.
[37] W. Zhang and L. M. Tolbert, "Survey of reactive power planning methods," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, San Francisco, CA, Jun. 12–16, 2005, pp. 1580–1590.
[38] U.S.-Canada Power System Outage Task Force, "Interim report: Causes of the August 14th blackout in the United States and Canada Nov. 2003.
[39] I. Balaguer, H. Kim, F. Z. Peng, and E. Ortiz, "Survey of photovoltaic power systems islanding detection methods," in *Proc. IEEE 34th Ind. Electron.*, Nov. 10–13, 2008, pp. 2247–2252.
[40] F. Z. Peng, Y. W. Li, and L. M. Tolbert, "Control and protection of power electronics interfaced distributed generation systems in a customer-driven microgrid," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Calgary, AB, Canada, Jul. 26–30, 2009.
[41] H. Qi, Y. Xu, and X. Wang, "Mobile-agent-based collaborative signal and information processing in sensor networks," *Proc. IEEE*, vol. 91, no. 8, pp. 1172–1183, Aug. 2003.
[42] H. Qi, S. S. Iyengar, and K. Chakrabarty, "Multi-resolution data integration using mobile agents in distributed sensor networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 31, pp. 383–391, Aug. 2001.
[43] L. Prasad, S. S. Iyengar, and R. L. Rao, "Fault-tolerant sensor integration using multiresolution decomposition," *Phys. Rev. E*, vol. 49, no. 4, pp. 3452–3461, Apr. 1994.
[44] L. Lamport, Digital System Research Center, "Synchronizing time servers," Tech. Rep. 18, 1987.
[45] H. Qi, W. Zhang, and L. M. Tolbert, "A resilient real-time agent-based system for a reconfigurable power grid," in *Proc. Int. Conf. Intell. Syst. Appl. Power Syst.*, Arlington, VA, Nov. 6–10, 2005.
[46] D. M. Falcao, F. F. Wu, and L. Murphy, "Parallel and distributed state estimation," *IEEE Trans. Power Syst.*, vol. 10, no. 2, pp. 724–730, May 1995.
[47] R. Ebrahimian and R. Baldick, "State estimation distributed processing," *IEEE Trans. Power Syst.*, vol. 15, no. 4, pp. 1240–1246, Nov. 2000.
[48] L. Xu, "Data modeling and processing in deregulated power system," Ph.D. dissertation, Washington State Univ., Pullman, WA, 2005.
[49] L. Xu, K. Tomsovic, and A. Bose, "Topology error identification using a two-state DC state estimator," *Elect. Power Syst. Res.*, vol. 74, no. 1, pp. 167–175, Apr. 2005.
[50] J. W. S. Liu, *Real-Time Systems*. Upper Saddle River, NJ: Prentice-Hall, 2000.
[51] X. Wang, D. Jia, C. Lu, and X. Koutsoukos, "DEUCON: Decentralized end-to-end utilization control for distributed real-time systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 7, pp. 996–1009, Jul. 2007.
[52] X. Wang, Y. Chen, C. Lu, and X. Koutsoukos, "FC-ORB: A robust distributed real-time embedded middleware with end-to-end utilization control," *J. Syst. Softw.*, vol. 80, no. 7, pp. 938–950, July 2007.
[53] C. Lu, X. Wang, and X. Koutsoukos, "Feedback utilization control in distributed real-time systems with end-to-end tasks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 16, no. 6, pp. 550–561, Jun. 2005.

Hairong Qi (S'97–M'00–SM'05) received the B.S. and M.S. degrees in computer science from Northern JiaoTong University, Beijing, China, in 1992 and 1995, respectively, and the Ph.D. degree in computer engineering from North Carolina State University, Raleigh, in 1999.

She is now a Professor in the Department of Electrical Engineering and Computer Science at the University of Tennessee, Knoxville. Her current research interests are robust collaborative processing in resource-constraint distributed environment and information unmixing. She has published over 100 technical papers in archival journals and refereed conference proceedings.

Dr. Qi is the recipient of the NSF CAREER award. She also received the Best Paper Awards from the 2009 ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC) and the 2006 International Conference on Pattern Recognition (ICPR). She serves on the editorial board of International Journal on Distributed Sensor Networks.

Xiaorui Wang (M'06) received the Ph.D. degree from Washington University in St. Louis in 2006.

He is an Assistant Professor at the University of Tennessee, Knoxville. He is an author or coauthor of more than 60 refereed publications.

Prof. Wang is a member of the IEEE Computer Society. He is the recipient of the U.S. Office of Naval Research (ONR) Young Investigator (YIP) Award in 2011 and the U.S. NSF CAREER Award in 2009. He also received the Best Paper Award from the 29th IEEE Real-Time Systems Symposium (RTSS) in 2008.

Leon M. Tolbert (S'88–M'91–SM'98) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Georgia Institute of Technology, Atlanta, in 1989, 1991, and 1999 respectively.

He worked in the Engineering Division, Oak Ridge National Laboratory, Knoxville, TN, from 1991 to 1999. He was appointed as an Assistant Professor in the Department of Electrical and Computer Engineering, University of Tennessee, Knoxville, in 1999. He is currently the Min Kao Professor in the Department of Electrical Engineering and Computer Science, University of Tennessee. He is also a Research Engineer with the Power Electronics and Electric Machinery Research Center, Oak Ridge National Laboratory. In 2010, he was a Visiting Professor at Zhejiang University, Hangzhou, China.

Dr. Tolbert is a Registered Professional Engineer in the state of Tennessee. He was the recipient of an NSF CAREER Award in 2001, the 2001 IEEE Industry Applications Society Outstanding Young Member, and three prize paper awards from the IEEE Industry Applications Society and IEEE Power Electronics Society. From 2003 to 2006, he was the Chairman of the Education Activities Committee of the IEEE Power Electronics Society and an Associate Editor for the IEEE POWER ELECTRONICS LETTERS. He has been an Associate Editor of the IEEE TRANSACTIONS ON POWER ELECTRONICS since 2007. He was elected to serve as a Member-At-Large to the IEEE Power Electronics Society Advisory Committee for 2010–2012.

Fangxing (Fran) Li (S'98–M'01–SM'05) received the B.S.E.E. and M.S.E.E. degrees from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Polytechnic Institute, Blacksburg, in 2001.

He worked at ABB, Raleigh, NC, as a Senior and then a Principal R&D Engineer from 2001 to 2005. Then he joined the University of Tennessee, Knoxville, in August 2005. His recent research interests include smart grids, renewable energy integration, and distributed generation control.

Dr. Li is a Registered Professional Engineer in the state of North Carolina and an Associate Editor of IEEE TRANSACTIONS ON SUSTAINABLE ENERGY.

Fang Zheng Peng (M'92–SM'96–F'05) received the B.S. degree in electrical engineering from Wuhan University, Wuhan, China, in 1983, and the M.S. and Ph.D. degrees in electrical engineering from Nagaoka University of Technology, Nagaoka, Japan, in 1987 and 1990, respectively.

From 1990 to 1992, he was a Research Scientist at Toyo Electric Manufacturing Company, Ltd., where he was involved in research and development of active power filters, flexible ac transmission system (FACTS) applications, and motor drives. From 1992 to 1994, he was a Research Assistant Professor at Tokyo Institute of Technology, Tokyo, Japan, where he initiated a multilevel inverter program for FACTS applications and a speed-sensorless vector control project. From 1994 to 2000, he was at Oak Ridge National Laboratory (ORNL), University of Tennessee, Knoxville, where he was a Research Assistant Professor during 1994–1997, and a Staff Member and the Lead (Principal) Scientist of the

Power Electronics and Electric Machinery Research Center during 1997–2000. In 2000, he joined Michigan State University, East Lansing, as an Associate Professor, where he is currently a Full Professor in the Department of Electrical and Computer Engineering. He holds more than ten patents.

Dr. Peng is a recipient of the 1996 First Prize Paper Award and the 1995 Second Prize Paper Award of the Industrial Power Converter Committee at the IEEE Industry Applications Society Annual Meeting, the 1996 Advanced Technology Award of the Inventors Clubs of America, Inc., International Hall of Fame, the 1991 First Prize Paper Award from the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, and the 1990 Best Paper Award from the *Transactions of the Institute of Electrical Engineers of Japan*, which is the Promotion Award of the Electrical Academy. He was the Chair of the Technical Committee for Rectifiers and Inverters of the IEEE Power Electronics Society from 2001 to 2005. From 1997 to 2001, he was an Associate Editor for the IEEE TRANSACTIONS ON POWER ELECTRONICS, and since 2005, he has been an Associate Editor for the same.

Peng Ning (M'03) received the B.S. degree in information science and the M.E. degree in communication and electronic systems from the University of Science and Technology, China, in 1994 and 1997, respectively, and the Ph.D. degree in information technology from George Mason University, Fairfax, VA, in 2001.

He is a Professor of Computer Science at North Carolina State University, Raleigh, where he also serves as the Technical Director for Secure Open Systems Initiative (SOSI) in College of Engineering.

Prof. Ning is a senior member of the ACM, the ACM SIGSAC, and a member of the IEEE Computer Society. He is a recipient of the National Science Foundation (NSF) CAREER award. He served or is serving on the editorial boards of ACM *Transactions on Sensor Networks*, *Journal of Computer Security*, *Ad-Hoc Networks*, *Ad-Hoc & Sensor Networks: An International Journal*, *International Journal of Security and Networks*, and *IET Proceedings Information Security*. He served as the Program Chair or Co-Chair of ICDCS-SPCC '10, ESORICS '09, ACM SASN '05, and ICICS '06, the General Chair of ACM CCS '07 and CCS '08, and Program Vice Chair for ICDCS '09 & '10—Security and Privacy Track. He is a Steering Committee member of ACM CCS and a founding Steering Committee member of ACM WiSec. He has served on the organizing committees or program committees for over sixty technical conferences or workshops related to computer and network security. His research has been supported by the NSF, the Army Research Office (ARO), the Advanced Research and Development Activity (ARDA), IBM Open Collaboration Research (OCR) program, SRI International, and the NCSU/Duke Center for Advanced Computing and Communication (CACC).

S. Massoud Amin (S'80–M'90–SM'00) received the B.S. degree with honors and the M.S. degree in electrical and computer engineering from the University of Massachusetts, Amherst, and the M.S. and D.Sc. degrees in systems science and mathematics from Washington University in St. Louis, MO.

He is leading extensive R&D efforts in smart grids and infrastructure security and is a leading expert on the U.S. electricity grid. Before becoming the Honeywell/H. W. Sweatt Chair in Technological Leadership, a Professor of Electrical and Computer Engineering, and a University Distinguished Professor at the University of Minnesota, he directed all infrastructure security, grid operations/planning, and energy markets at the Electric Power Research Institute (EPRI) after 9/11. Prior to that he led mathematics and information sciences at EPRI, worked on self-repairing energy infrastructures, coined the term "smart grid" in 1998, is considered as the "father of smart grid," and led the development of over 24 technologies transferred to industry. He is the coauthor of over 190 publications, editor of 7 collections, and serves on several boards.

Prof. Amin was three times Professor of the Year at Washington University, is a fellow of the ASME, received several awards at EPRI, including the 2002 President's Award, and twice received Chauncey Awards, the institute's highest honor.